PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 :
G06K 7/08, 7/10, 19/12
G06K 19/16

A1

(11) International Publication Number: WO 93/12506

(43) International Publication Date: 24 June 1993 (24.06.93)

(21) International Application Number: PCT/US92/10357

(22) International Filing Date: 1 December 1992 (01.12.92)

(30) Priority data:

810,483	19 December 1991 (19.12.91)	US
857,729	26 March 1992 (26.03.92)	US
921,460	28 July 1992 (28.07.92)	US

(71) Applicant: CONTROL MODULE INC. [US/US]; 380 Enfield Street, Enfield, CT 06082 (US).

(72) Inventors: BIANCO, James, S. ; 217 Brainard Road, Enfield, CT 06082 (US). HORAN, David, J. ; 100 Loomis Ridge, Westfield, MA 01085 (US). DRUMMOND, Bernard ; 30 Ed Holcomb Road, Southwick, MA 01077 (US). VANGEL, Peter, D. ; 54 Lathrop Street, South Hadley, MA 01075 (US).

(74) Agent: CROZIER, John, H.; 1934 Huntington Turnpike, Trumbull, CT 06611-5116 (US).

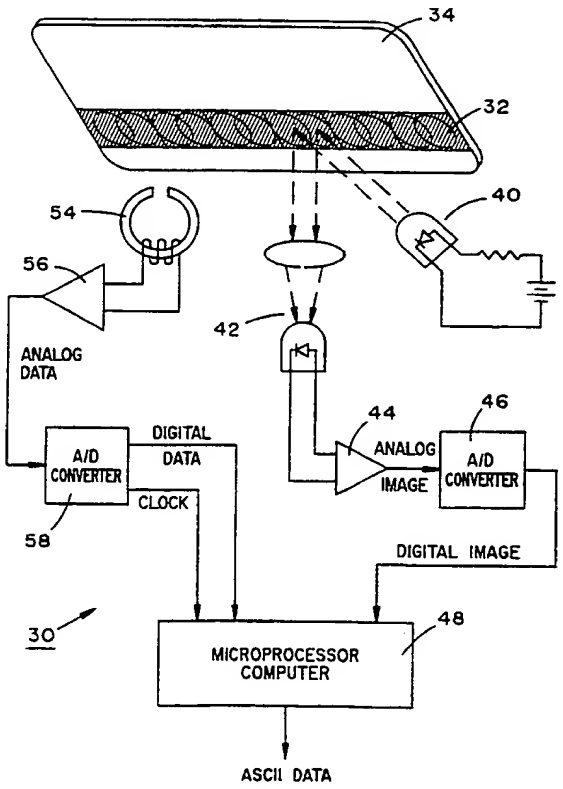
(81) Designated States: AU, BB, BG, BR, CA, CS, FI, HU, JP, KP, KR, LK, MG, MN, MW, NO, NZ, PL, PT, RO, RU, SD, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE OPTOMAGNETIC IDENTIFICATION

(57) Abstract

In a preferred embodiment, a method of providing a security code for an identification document having thereon magnetically encoded information and a holographic image (32), including: optically reading (40) the holographic image and magnetically reading (54) the magnetically encoded information, providing relative position information by determining the position of the holographic image relative to the position of the magnetically encoded information, encrypting the relative position information, and magnetically encoding the relative position information on the identification document. The identification document having the relative position information thereon is provided, as well as a method and system for decoding such identification document.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NL	Netherlands
BE	Belgium	GN	Guinea	NO	Norway
BF	Burkina Faso	GR	Greece	NZ	New Zealand
BG	Bulgaria	HU	Hungary	PL	Poland
BJ	Benin	IE	Ireland	PT	Portugal
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SK	Slovak Republic
CI	Côte d'Ivoire	KZ	Kazakhstan	SN	Senegal
CM	Cameroon	LI	Liechtenstein	SU	Soviet Union
CS	Czechoslovakia	LK	Sri Lanka	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	MC	Monaco	UA	Ukraine
DK	Denmark	MG	Madagascar	US	United States of America
ES	Spain	ML	Mali	VN	Viet Nam
FI	Finland	MN	Mongolia		

Description

Secure Optomagnetic Identification

Technical Field

The present invention relates to identification means generally and, more particularly, but not by way of limitation, to a unique identification method and means that combines encoded optical and magnetic information.

Background Art

As the need for more unattended credit card use expands, there is a greater need to verify the authenticity of the credit card to which the transaction is being charged.

One of the major methods used by forgers of credit cards is to obtain the numbers encoded on a valid credit card during a legitimate transaction and, at a later time, to include this number on another credit card. When the forged credit card is subsequently used on a transaction, the charge is applied to the valid number and the account of the owner of the valid credit card is charged accordingly. The only way to prevent this type of theft is to computer validate each transaction as the purchase is taking place and to have a cashier check the identification of the person purchasing the items against the name returned by the validation computer. While this procedure is economically justifiable when the purchase is for a relatively large amount and

there is a cashier present, it is impossible to use this method for small transactions such as with vending machines, pay telephone, transit charges, automatic teller machines, and a host of other unattended charge applications.

There have also been elaborate attempts to create graphic patterns embellished with holographic photographic images to prevent forged credit cards from easily being produced. However, with today's high-tech criminal element, credit cards and holographic images can be illegally produced and sold at high profits. In addition, this method of security still depends on the human element to inspect the card and identify the holder and to cancel the transaction, if necessary, something not appreciated by most physically exposed cashiers or clerks.

A further problem with conventional credit cards is that the embossed indicia thereon, usually numbers, are subject to tampering. For example, the upper righthand loop of an "8" may be flattened to simulate a "6" to produce a bogus number. When read with a mechanical reader without verification, the bogus number will be recorded when the transaction is completed.

Accordingly, it is a principal object of the present invention to provide identification method and means to ensure that an identification is authentic and not a forgery and to make this verification without human intervention.

It is a further object of the invention to provide such method and means that makes it extremely difficult to duplicate or forge identification means.

It is an additional object of the invention to provide such method and means that is economical.

It is another object of the invention to provide such method and means that does not require host computer support.

It is yet a further object of the invention to provide such method and means that produce identification means that can provide conventional information to conventional identification readers.

It is yet an additional object of the invention to provide method and means to indicate tampering with embossed indicia.

Other objects of the present invention, as well as particular features, elements, and advantages thereof, will be elucidated in, or be apparent from, the following description and the accompanying drawing figures.

Disclosure of Invention

The present invention achieves the above objects, among others, by providing, in a preferred embodiment, a method of providing a security code for identification means having thereon magnetically encoded information and a holographic image, including: optically reading said holographic image and magnetically reading said magnetically encoded information, providing relative position information by determining the position of said holographic image relative to the position of said magnetically encoded information, encrypting said relative position information; and, magnetically encoding said relative position information on said identification means. Identification means having said relative position information thereon is provided, as well as method and means for decoding such identification means.

Brief Description of Drawings

Understanding of the present invention and the various aspects thereof will be facilitated by reference to the accompanying drawing figures, submitted for purposes of illustration only and not intended to define the scope of the invention, in which:

Figure 1 is a front elevational view of a conventional identification card.

Figure 2 is a rear elevational view of a conventional identification card.

Figure 3 is a rear elevational view of a conventional identification card.

Figure 4 is a schematic diagram illustrating a system reading an identification card according to the present invention.

Figure 5 illustrates the treatment of data read by the system of Figure 4.

Figure 6 is a rear elevational view of an identification card showing the arrangement of magnetic information thereon.

Figure 7 illustrates the logic diagram for encoding the security portion of the card of Figure 6.

Figure 8 illustrates the logic diagram for decoding the security portion of the card of Figure 6 encoded according to the method of Figure 7.

Figure 9 illustrates the logic diagram for encoding the security portion of the card of Figure 6 according to an alternative method.

Figure 10 illustrates the logic diagram for decoding the security portion of the card of Figure 6 encoded according to the method of Figure 9.

Figure 11 is a front elevational view of another type of conventional identification card.

Figure 12 is a front elevational view of the identification card of Figure 11 modified in accordance with another aspect of the present invention.

Figure 13 is a front elevational view of the identification card of Figure 11 modified in accordance with a further aspect of the invention.

Figure 14 is a schematic diagram showing a light beam being reflected from a mirrored surface.

Figure 15 is a schematic diagram showing a light beam being diffracted by a diffraction grating.

Figure 16 is a schematic diagram showing a light beam being diffracted by a diffraction grating.

Figure 17 is a schematic diagram showing a light beam being diffracted by a hologram.

Figure 18 is a schematic diagram showing the detection of a light beam being diffracted by a diffraction grating.

Figure 19 is a schematic diagram showing the detection of a light beam being diffracted by a diffraction grating.

Figures 20A-20C are schematic diagrams illustrating the detection of a light beam diffracted by a diffraction grating and the output signals produced thereby.

Figures 21A-21C are schematic diagrams illustrating the process of copying a diffraction grating.

Figures 22A-22C are schematic diagrams illustrating the detection of two light beams diffracted by a compound diffraction grating and the output signals produced thereby.

Figures 23A-23C are schematic diagrams illustrating the detection of two light beams diffracted by a compound diffraction grating with a holographic image placed thereon and the output signals produced thereby.

Best Mode for Carrying Out the Invention

Reference should now be made to the drawing figures, in which similar or identical elements are given consistent identifying numerals throughout the various figures thereof, and in which parenthetical references to figure numbers direct the reader to the view(s) in which the element(s) being described is (are) best seen, although the element(s) may be seen also in other views.

Figure 1 illustrates the rear of a conventional identification, or credit, card 10 containing a magnetic stripe 12 in which is encoded information as is more fully described below.

Figure 2 illustrates the front of card 10 containing a holographic image 14 which is intended to identify the card as being authentic.

Figure 3 illustrates the rear of a recently developed identification, or credit, card 20 containing an optomagnetic stripe 22 comprising a magnetic stripe, as above, directly overprinted with a holographic image, as above. The purpose of the composite stripe is to make counterfeiting of such cards more difficult.

As is noted in more detail below, when cards 10 and 20 are credit cards, the magnetic stripe will be encoded according to American Banking Association protocols which provide particular information in a predetermined format, so that conventional magnetic

readers will be able to decode the information to determine the issuing institution, the user's account number, expiration date, etc.

Figure 4 illustrates a system, according to the present invention, generally indicated by the reference numeral 30, reading a composite optomagnetic stripe 32 on a credit card 34. System 30 includes a light source 40 disposed so as to illuminate optomagnetic stripe 32. A pattern of more and less reflective regions of stripe 32 is detected by a photodetector and the resulting analog signals representing the pattern are amplified by an amplifier 44. The analog signals are converted to digital signals in an analog-to-digital converter 46 and the resulting digital representation of the pattern is passed to a microprocessor 48.

Simultaneously, a magnetic detector 54 in proximity to optomagnetic stripe 32 produces a stream of analog data from encoded in the magnetic portion of the stripe, which analog data is amplified in an amplifier 56. The analog data signal is converted to digital signal in an analog-to-digital converter 58 and is passed to microprocessor 48. In a similar manner, a digital clock pulse is read from the magnetic portion of optomagnetic stripe 32 and is passed to microprocessor 48. Data from microprocessor 48 relative to the credit card transaction may be sent to a host computer (not shown) in ASCII format.

The holographic image portion of each optomagnetic stripe 32 is not placed in precisely the same location on each card 34; therefore, by determining the pattern of the holographic image with respect to the encoded magnetic information, provides an indication of whether the card is a forgery. The means for determining the location of this pattern is

indicated on Figure 5. As indicated on Figure 4, the holographic image is read to produce an analog pattern of more and less reflective areas of the hologram. Unlike the conventional optical reading of a sharply defined bar code, the hologram produces a relatively undefined analog holographic image. Once this is passed through analog-to-digital converter 46, the sharply defined digital holographic image is produced. The magnetic data and the magnetic clock pulses are similarly converted to sharply defined digital pulse trains. Now, at the leading edge of each clock pulse, the digital holographic image and the magnetic data are read and accumulation of such readings is a representation of the pattern of the holographic image with respect to the magnetic coded date on composite stripe 32. This accumulated pattern data is encrypted and encoded on the magnetic portion of stripe 32 and is used for card authentication, as will be described in more detail below.

As a further security measure, the magnetic portion of composite stripe 32 may be encoded with a special code as is described in US Patent Application No. 07/569,232, filed August 17, 1990, which is a continuation of US Patent Application No. 07/338,373, filed April 13, 1989, now abandoned, by James S. Bianco, titled IDENTIFICATION MEANS WITH ENCRYPTED SECURITY CODE AND METHOD OF MAKING AND USING SAME, the disclosures of which applications are incorporated by reference hereinto. As described in the foregoing applications, a magnetic portion of composite strip 32 may include a security code formed by the encryption of some information otherwise in the magnetic portion, such as the user's identification number, with a password. When the security code is decoded with a reader having the password, if the identification

number is produced, there is an additional indication that card 34 is valid.

Referring now to Figure 6, there is shown card 34 with the holographic portion of composite stripe 32 removed to indicate the locations of the various types of magnetic information stored therein. Stripe 32 normally contains at least two tracks of information, here, tracks 70, and 72. The technique employed is a two-frequency, coherent-phase, recording technique which allows serial recording of self-clocking data on a single track. When the data is decoded, a clock pulse train is produced in addition to the data information.

Since the ABA encodement does not consume the entire length of stripe 32, a portion of the tracks on the stripe may be used for storing additional information, here, portions 70' and 72' which are used to store the holographic pattern and the security code noted above. Stripe 32 has conventional dead zones 80 and 82 at the ends thereof, so that card 34 can be read from either direction. Likewise, a conventional dead zone 84 is provided between the ABA and security portions of stripe 32.

Figure 7 illustrates the method by which the security portion of composite stripe 32, i.e., tracks 70' and 72', is encoded. A password and the user ID number are encrypted with a special algorithm to produce a security code which is then recorded in the security portion of stripe 32. The digital signals from reading of the holographic and magnetic portions of stripe 32 (Figure 4) are combined to produce a pattern identification which is also recorded in the security portion of stripe 32.

Figure 8 illustrates the method by which card 34 is read to determine the validity thereof. The security code is read and decoded with the password stored in the reader with a special decoding algorithm. The result is compared with the stored password and, if they are not identical, the card is invalid and the transaction may be terminated. The holographic pattern is determined, as is described with reference to Figure 4. The currently read pattern is compared with the pattern recorded in the security portion of stripe 32. If the two patterns are not identical, the card is invalid and the transaction may be terminated. Only if both comparisons are identical will the card be determined to be valid. Thus, the present invention provides two levels of security, either one of which is extremely difficult to forge.

An alternative method of encoding security data is shown on Figure 9. Here, the password, the user ID number, and the holographic pattern information are encryted to produce the security code. Similarly, the decoding sequence shown on Figure 10 decodes the security code, and if the password is obtained, the pattern information is compared to the currently read pattern. If the later comparison is favorable, the card is valid. Alternatively, the pattern information could first be compared and then the passwords.

A particular advantage of the present invention is that the magnetically encoded ABA information can be read by a conventional magnetic reader. When additional verification is desired, the special reading system shown on Figure 4 can be employed.

It is also within the contemplation of the present invention to employ any type of visual image on an identification, or credit, card, such as a photograph or such as bar code as is shown on Figure 11 where a bar code 100 disposed on a card 120 having also disposed thereon a magnetic stripe 122. The location of bar code 100 with respect to magnetic stripe 122 would be encoded in the magnetic stripe as is described above with reference to a hologram. Bar code 110 can, of course, have additional information encoded therein.

Figure 12 illustrates a conventional identification card 220 on which there is disposed a hologram 222 which may be superimposed over a magnetic stripe (not shown) and on which there is embossed a line of numbers, generally indicated by the reference numeral 224.

Figure 13 illustrates an identification card 220' which is card 220 of Figure 12 modified by the addition of holographic image 230 disposed over line of numbers 224'. Holographic image 230 may be a separate strip, as shown on Figure 13, or strip 222' may be provided wide enough to cover a magnetic stripe and line of numbers 224'.

Provision of holographic image 230 over line of numbers 224 will not, in itself, prevent or detect tampering. However, if line of numbers 224' has been tampered with, image 230 will be distorted and, when card 220' is read with system 30 of Figure 4, the card will be identified as being a forgery or having been tampered
with.

While the term "image" has been used herein and in the appended claims, the term is not being used in its strict sense of being a representation of a person or thing, but, rather, the term is being used to describe any optically readable pattern, whether representative of a person or thing.

A further aspect of the present invention provides an even higher level of security.

With today's advanced technology, it is possible to forge or duplicate any security device, should the forger have enough time and money available. The recent flood of false credit cards with their identical holomagnetic seals is testimony to the cleverness and fortitude of unscrupulous forgers. These cards are produced at a low expense, typically little more than their original counterparts. They are easily encoded with valid account numbers which have been skimmed from unsuspecting credit card users. To combat this problem, the holomagnetic security media has been developed.

The holomagnetic media combines the optical imagery of holographics, diffraction gratings and magnetic oxide to produce a machine-readable media that is very difficult to replicate. However, as it was stated earlier, it is still possible to duplicate a holographic image and reproduce it on a magnetic oxide layer. To do this would be a very expensive proposition requiring very sophisticated laser and optical equipment in addition to a powerful computer and a thorough knowledge of physics and optics.

The holomagnetic security feature of the present invention is based on an optical image that is generated by the combination of two different optical gratings and spacial holographic images, with all components placed in a random pattern. The master

image is produced on a large holographic dye which produces millions of unique holographic credit cards.

Because each card has a unique optical image which is associated with its encoded magnetic data, it is necessary for the forger to copy not only the magnetic data unique to the account data, but also the optical information that is also unique to the account data. No longer can the forger produce a large volume of fraudulent credit cards which can be embossed or encoded with any account number. It now is necessary for the forger to produce a unique card for each forged account. Because the forger must produce a unique card for each account, it is no longer economical for the forger to spend thousands of dollars to produce one card. The cost to produce this card would not cover the amount that could be stolen and, therefore, the forgery is not worth the risk.

To understand how the holomagnetics of the present invention achieve this uniqueness, it is necessary to discuss each of the technologies involved.

When a beam of light strikes a mirrored surface, it will reflect at the angle A2, as is shown on Figure 14. The reflected angle A2 is equal to the incident angle A1. When the incident angle A1 is changed, the reflection angle A2 will change proportionately. However, as shown on Figure 15, when that same beam of light strikes a diffraction grating, it will be diffracted into one or more beams of light. The diffracted angles are based on a number of variables. The variables which affect the angles are the size, and spacing of the grating and its form and the wave length of the source of light. On Figure 16, the grating spacing (d2), the incident angle (a7), and the wave length of the light source are changed. Thus, a

different set of diffracted light will be generated, again creating one or more shafts of diffracted light. These angles of diffracted light are mathematically predictable.

As shown on Figure 17, when the mirrored surface is pressed with the holographic cast, it will form a typographical characteristic. When a light source of single wave length component strikes the holographic surface, one or more bands of light will be generated. The location of these bands of light will vary depending on the form of holographic image used. Because of the complexity of the holographic form, predicting where these bands will fall is very difficult. It is these unique optical properties that are used to develop the security features of the holomagnetic tape of the present invention.

A holographic reader, in its basic form, contains a single light source 300 and a single detector 302, as shown on Figure 18, reading a holographic image, or diffraction grating, 304. The placement of light source 300 and detector 302 may be either as shown on Figure 18 or as on Figure 19. Figures 20A-C show the effects of a single light source 300 and detector 302 reading holographic image 304. Figure 20 shows the effects of a single light source and detector reading holographic image 304. Figure 20A depicts holomagnetic image 320 placed on a credit card 322, the image being created by piecing together a number of standard optical grating segments. Each segment is cut from a standard pattern having a grating dimension of D1; however, the widths of the segments and the angles of rotation of the segments are varied. As shown on Figure 20A, segment 1 is made up of grating lines which are perpendicular to the base of credit card 322. Segment 2's grating

lines are rotated at a 40 degree angle. Segment 3's grating lines are rotated at an 80 degree angle. In segment 4, the original zero degree grating is again used. It can be seen that the widths of the segments varies also. This varying of angles and widths produces a holographic tape of random patterns, all using the same master grating with D1 dimension.

When credit card 322 is passed through a holographic authorization reader utilizing a single light source 300 and detector 302 as shown on Figures 18 and 20A, two signals will be generated when the holographic tape is read. These signals are shown on Figure 20C. When credit card 322 is moved from the right to the left, a beam of diffracted light will be detected each time the zero grating enters the light beam. These signals are shown on Figure 20C as A (analog) and A' (digital). When the areas in segments 2 and 3 pass by the optical viewing area, the diffraction beams are either deflected to a different location or are not generated at all. Thus, there is no analog signal output. However, when segment 4 passes the optical viewing area, an analog signal again is generated. This time it is of longer duration. When used with a magnetic media, as described above, the magnetic coded data generates a coincident data clock. This example is a holomagnetic media in its basic form.

If, in the authorization terminal, single light source 300 and detector 302 were used to read the media, it would be possible for a forger to develop a pseudo-image on a forged credit card that would produce the same results. To do this, the forger would produce a credit card which was hot-stamped with an optical magnetic tape made by using a standard optical grating across the entire tape as shown on

Figure 21A, where a grating 350 is shown on a credit card 352. The forger then would modify a standard authorization terminal so as to capture the optical image generated by a holomagnetic credit card, as well as the magnetically encoded account information, as shown on Figure 21B.

The forger now can take the recorded data and, through the use of a very sophisticated computer and laser etching system, reconstruct a holomagnetic image on a false credit card that would fool the authorization terminal. The forger would achieve this by removing the grating in the area of segments 2, 3, 5, 6, and 8, as shown on Figure 21C. This forged card would produce the same results as the original; however, it still would be costly even to produce this card.

To make it extremely difficult to forge a holomagnetic card, the present invention equips the holomagnetic reader with two light sources and two detectors, as shown on Figure 22B, where a first light source and detector 360 and 362, respectively, and a second light source and detector 364 and 366, respectively, are shown reading a holographic tape 380 on a credit card 382. First light source and detector 360 and 362 operate in the visible light range, while second light source and detector 364 and 366 operate in the infrared light range. The combination creates a dual sensor holographic reader.

To support the dual image concept, a holographic tape 380 on a credit card 382 as shown on Figure 22A, is produced by mixing two different gratings. The dimension of the first grating is D1, while the dimension of the second grating is D2. The grating segments are located again at different angles and have different widths to form a random pattern. Thus,

we have produced an optical media which uses different gratings, different widths, and different angular rotation.

When credit card 382 is passed through a holomagnetic reader (Figure 22B), two sets of analog signals are generated. The original A and A' signals as shown on Figure 20C are again produced as on Figure 22C. In addition, a second set of signals which are B and B' are generated from the second channel. Because the B signals are generated from the D2 gratings, they are not in phase with the A signals generated by the D1 gratings. The viewing areas for both the A and the B channels are in the same track; however, they are spaced apart from one another. This produces two unique optical signatures for the same path on the holomagnetic tape. Again, there is a magnetic clock generated by the encoded data.

In order to produce a forged optical image that would generate the same results as the holomagnetic tape of Figure 22A, it would be necessary to start with a tape that contains both diffraction gratings D1 and D2. Because of the unique properties of the diffraction gratings, it would be virtually impossible to make a grating that would give the same results as 380 on Figure 22. If a grating with D1 spacing were modified to make a grating that would give the D1 results, it would not be possible to produce the D2 results. The only way possible to duplicate the optical image that is produced by the random pattern gratings, is to photograph the original card holographically and to generate a holographic die. Next, one would create a holographic foil by casting this holographic die into the foil at exactly the right place so that it would line up with the original magnetic data, for the relationship between the

optical image and the magnetic data must be maintained. It is obvious that this process would be very costly to produce a single fraudulent credit card and this process would have to be repeated for each fraudulent credit card produced.

To further complicate matters for the forger, it is possible to superimpose a holographic spacial image on the gratings. This is shown on Figure 23A, where holographic spacial image 400 is superimposed over holographic image 380. When this complex image is viewed by the electronic circuitry of Figure 23B, it would produce a very complex signature, as shown on Figure 23C, and it would be nearly impossible for a forger to reproduce a holomagnetic image that would produce the same results. In any case, it would be extremely expensive and time-consuming. Again, only a single credit card would be produced.

The reading elements of system 30 (Figure 4) are conventional and the system may be economically constructed therefrom. Microprocessor 48 may be programmed by conventional methods to provide the required functions.

It will thus be seen that the objects set forth above, among those elucidated in, or made apparent from, the preceding description, are efficiently attained and, since certain changes may be made in the above construction without departing from the scope of the invention, it is intended that all matter contained in the above description or shown on the accompanying drawing figures shall be interpreted as illustrative only and not in a limiting sense.

It is also to be understood that the following claims are intended to cover all of the generic and specific features of the invention herein described and all statements of the scope of the invention

which, as a matter of language, might be said to fall therebetween.

Claims

1. A method of providing security for identification means having thereon magnetically encoded information and a optically readable pattern, comprising:

(a) optically reading said optically readable pattern and magnetically reading said magnetically encoded information;

(b) providing relative position information by determining the position of said optically readable pattern relative to the position of said magnetically encoded information on said identification means; and

(c) magnetically encoding said relative position information on said identification means.

2. A method, as defined in Claim 1, further comprising the step of encrypting said relative position information with a security code prior to said encoding step.

3. A method, as defined in Claim 1, including:

(a) reading said optically readable pattern with a photodetector and digitizing the output thereof;

(b) reading said magnetically encoded information with a magnetic detector and digitizing the output thereof; and

(c) encrypting said digitized outputs with a security code by means of a microprocessor prior to said encoding step.

4. A method, as defined in Claim 1, further comprising providing as said optically readable pattern a holographic image.

5. A method, as defined in Claim 1, further comprising providing as said optically readable pattern a bar code.

6. A method, as defined in Claim 1, further comprising providing as said optically readable pattern a first diffraction grating.

7. A method, as defined in Claim 1, further comprising providing as said optically readable pattern first and second diffraction gratings.

8. A method, as defined in Claim 1, further comprising providing as said optically readable pattern a holographic image superjacent a diffraction grating.

9. A method, as defined in Claim 7, including:

(a) optically reading said first diffraction grating with a first photodetector and providing an output representative of said first diffraction grating; and

(b) optically reading said second diffraction grating with a second photodetector and providing an output representative of said second diffraction grating.

10. A method, as defined in Claim 1, further comprising providing as said optically readable pattern a holographic image superjacent embossed indicia and said method includes detecting tampering with said embossed indicia by determining if said holographic image is distorted.

11. An apparatus for optically reading an optically readable diffraction pattern, comprising:

(a) a first light source to direct a beam of light against said optically readable diffraction pattern; and

(b) a first photodetector to receive light from said first light source diffracted by a first portion of said optically readable diffraction pattern and to produce a signal representative of said first portion of said optically readable diffraction pattern as said first photodetector and said optically readable diffraction pattern are moved relative to each other.

12. An apparatus, as defined in Claim 11, wherein said optically readable diffraction pattern comprises first and second diffraction gratings, said first portion of said optically readable diffraction pattern is said first diffraction grating, and said apparatus further comprises:

(a) a second light source to direct a beam of light against said optically readable diffraction pattern; and

(b) a second photodetector to receive light from said second light source diffracted by said second diffraction grating and to produce a signal representative of said first portion of said optically readable pattern as said first photodetector and said optically readable diffraction pattern are moved relative to each other.

13. An apparatus, as defined in Claim 11, wherein said optically readable diffraction pattern comprises a holographic image.

14. An apparatus, as defined in Claim 11, wherein said optically readable diffraction pattern includes a diffraction grating with a superjacent holographic image.

15. An apparatus, as defined in Claim 12, wherein said optically readable diffraction pattern includes a holographic image superjacent said first and second diffraction gratings.

16. An apparatus, as defined in Claim 11, wherein said optically readable diffraction pattern includes a holographic image superjacent embossed indicia.

17. Secure identification means, comprising:

(a) an optically readable pattern disposed on said identification means;

(b) magnetically encoded information disposed on said identification means; and

(c) said magnetically encoded information including therein information as to the relative position of said optically readable pattern with respect to said magnetically encoded information.

18. Secure identification means, as defined in Claim 17, wherein at least a portion of said magnetically encoded information is encrypted with a security code.

19. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises a holographic image.

20. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises a bar code.

21. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises a first diffraction grating.

22. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises first and second diffraction gratings.

23. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises a holographic image superjacent a diffraction grating.

24. Secure identification means, as defined in Claim 17, wherein said optically readable pattern comprises a holographic image superjacent embossed indicia.

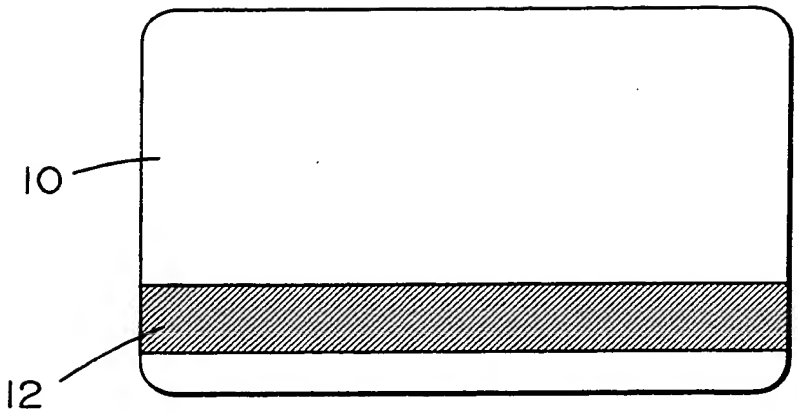


FIG. 1
(PRIOR ART)

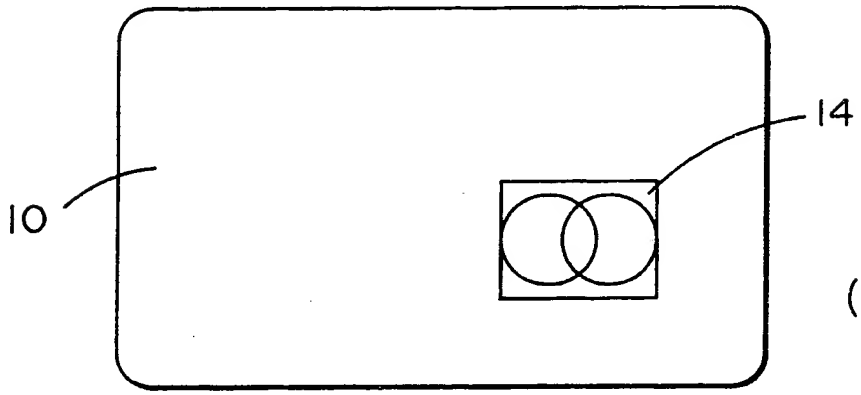


FIG. 2
(PRIOR ART)

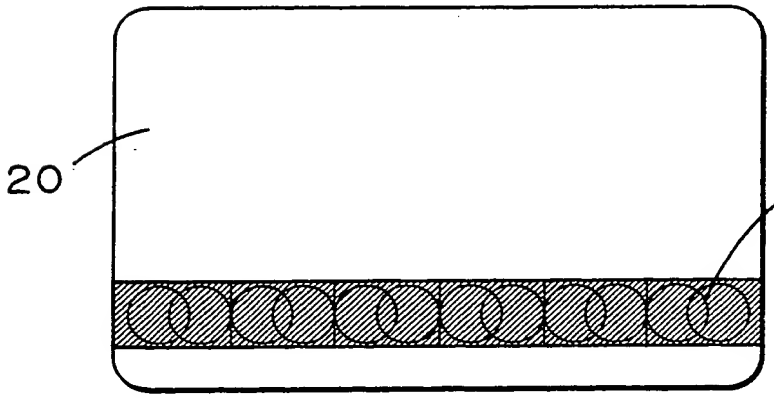


FIG. 3
(PRIOR ART)

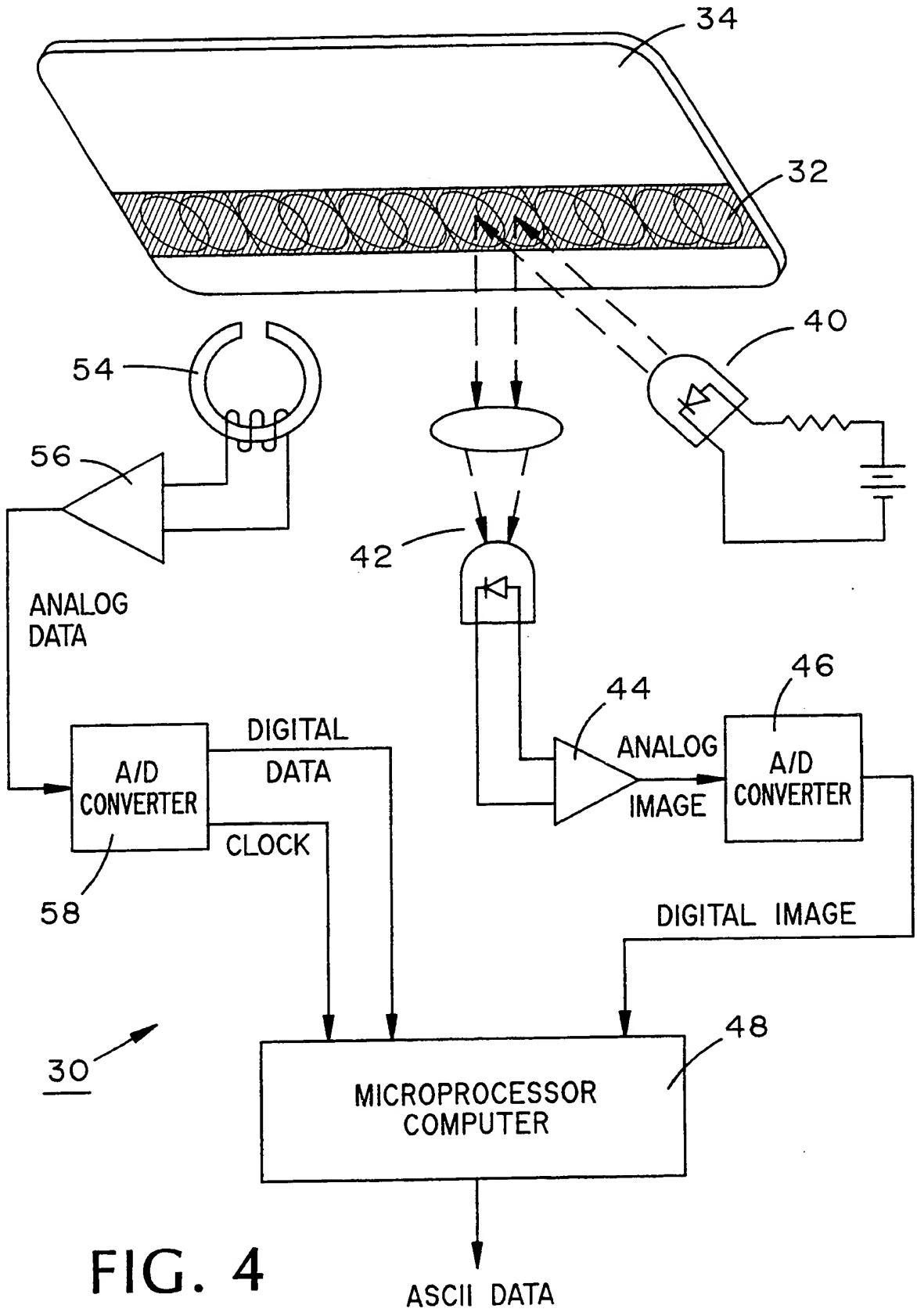


FIG. 4

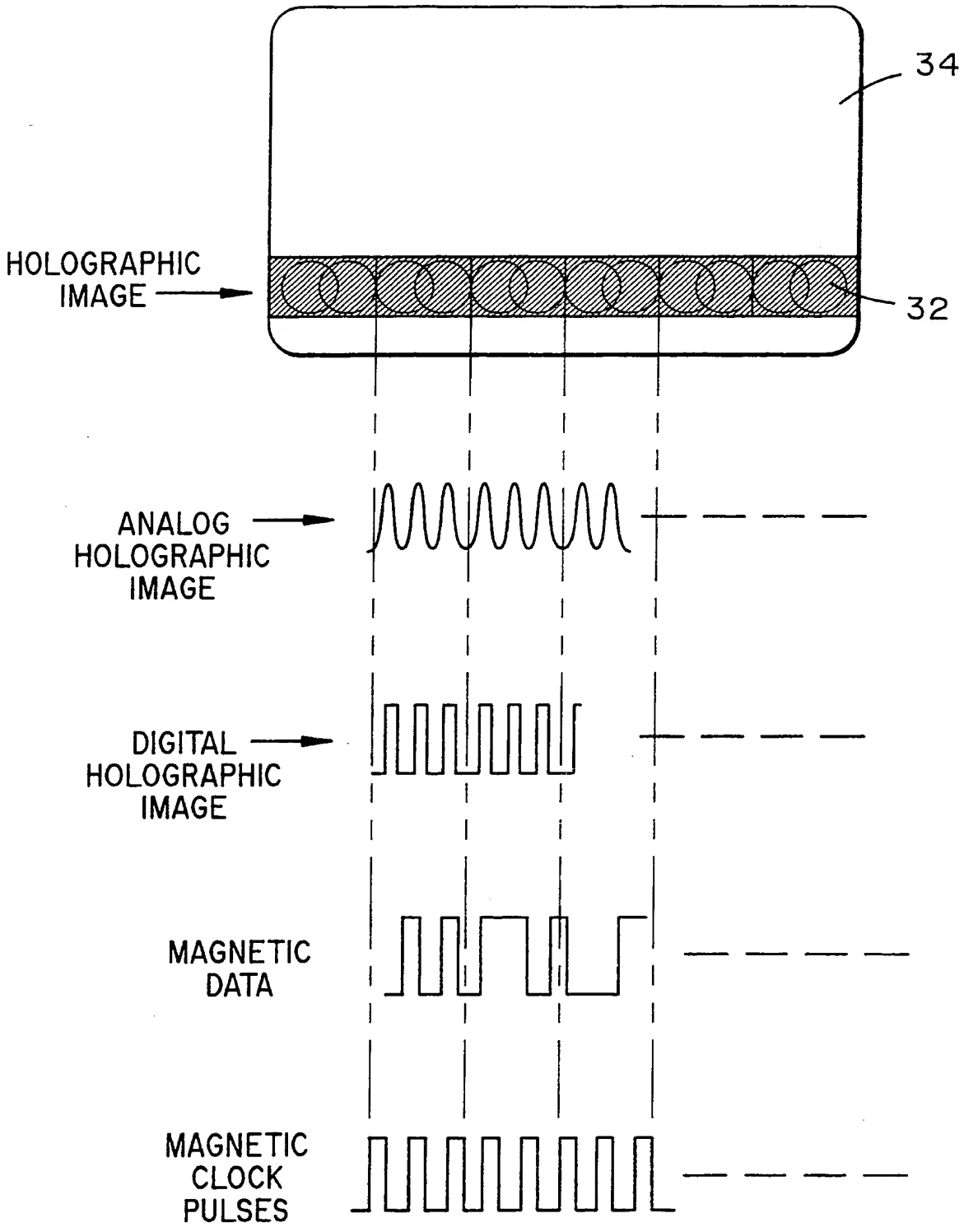


FIG. 5

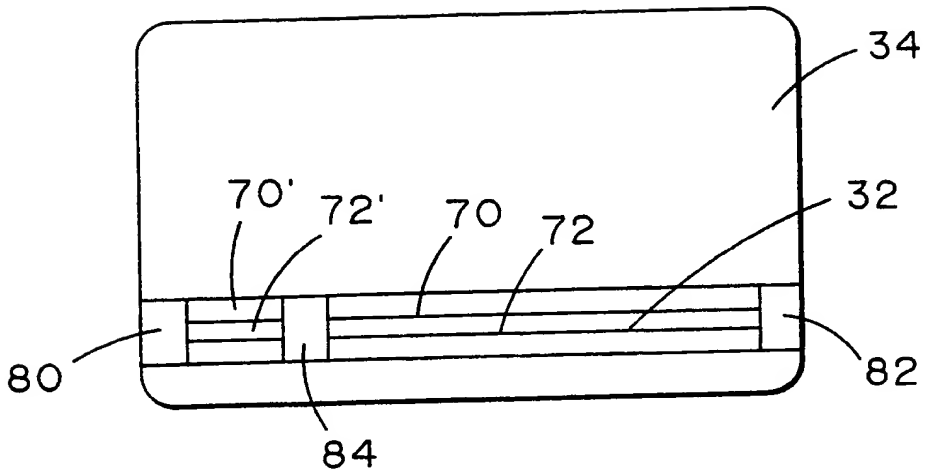


FIG. 6

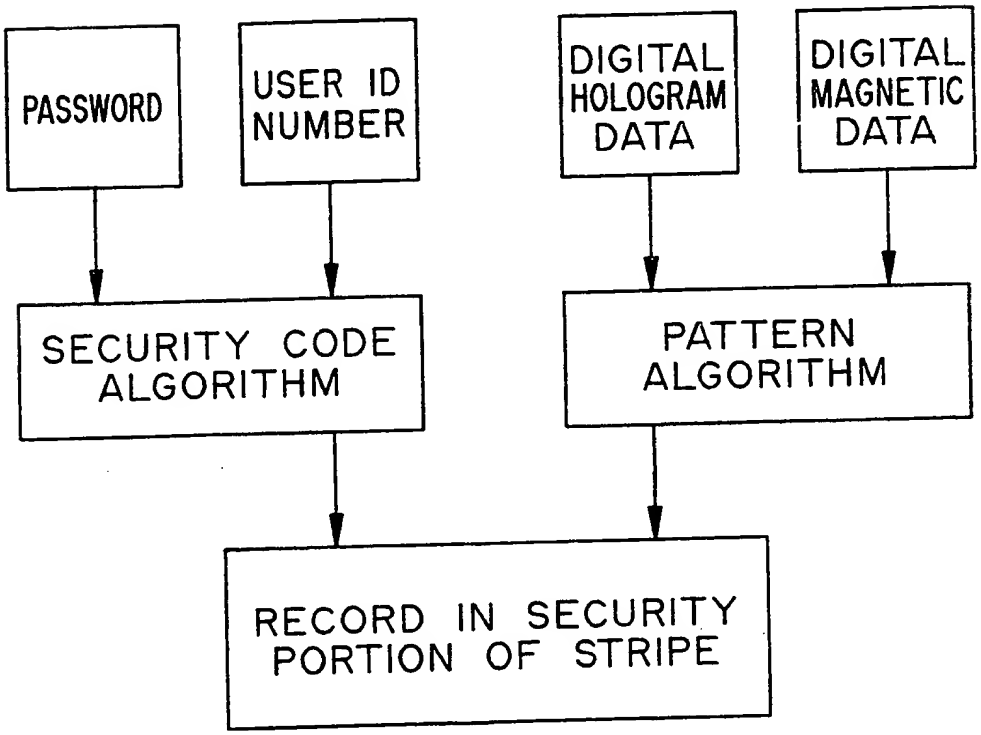


FIG. 7

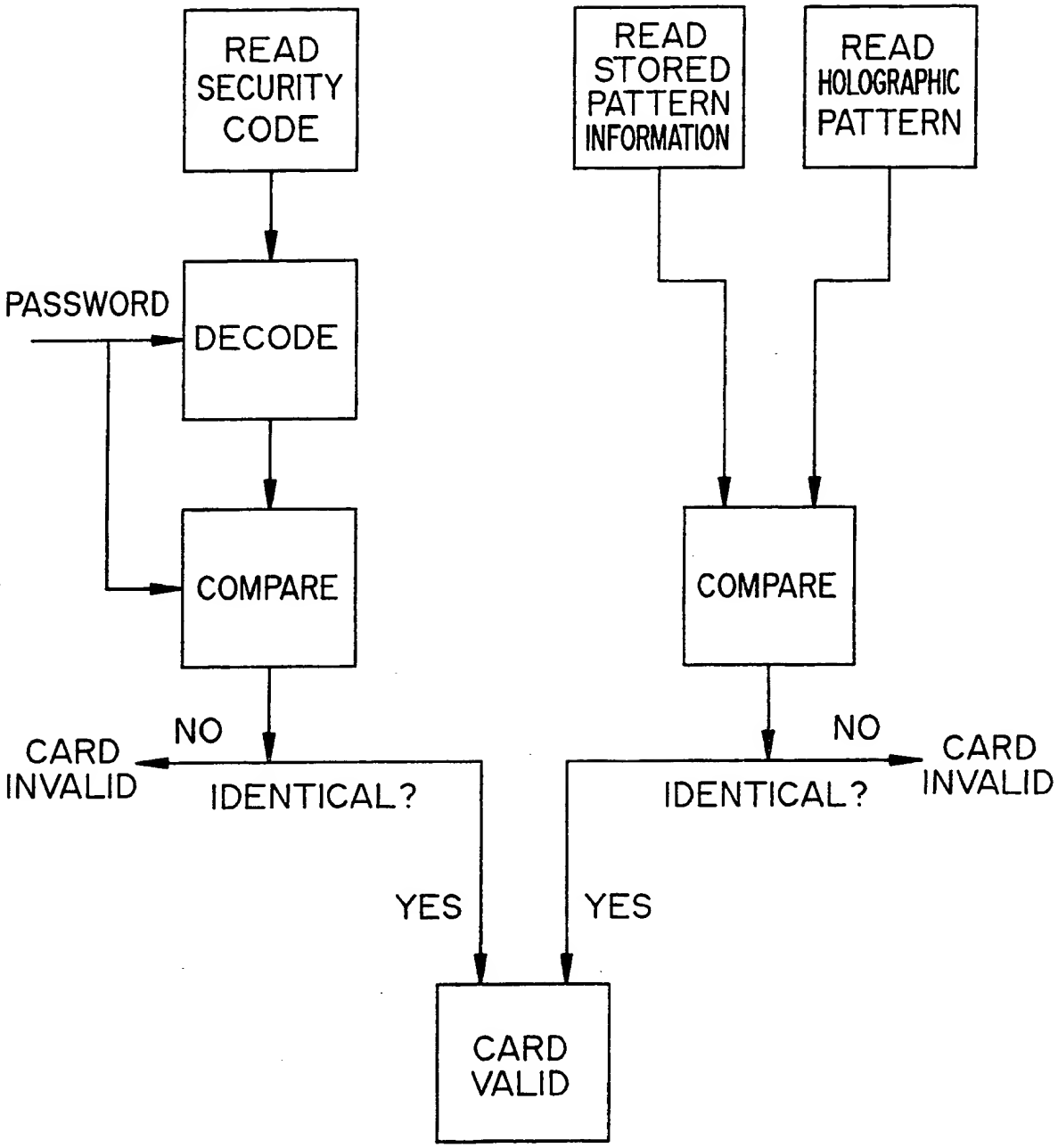


FIG. 8

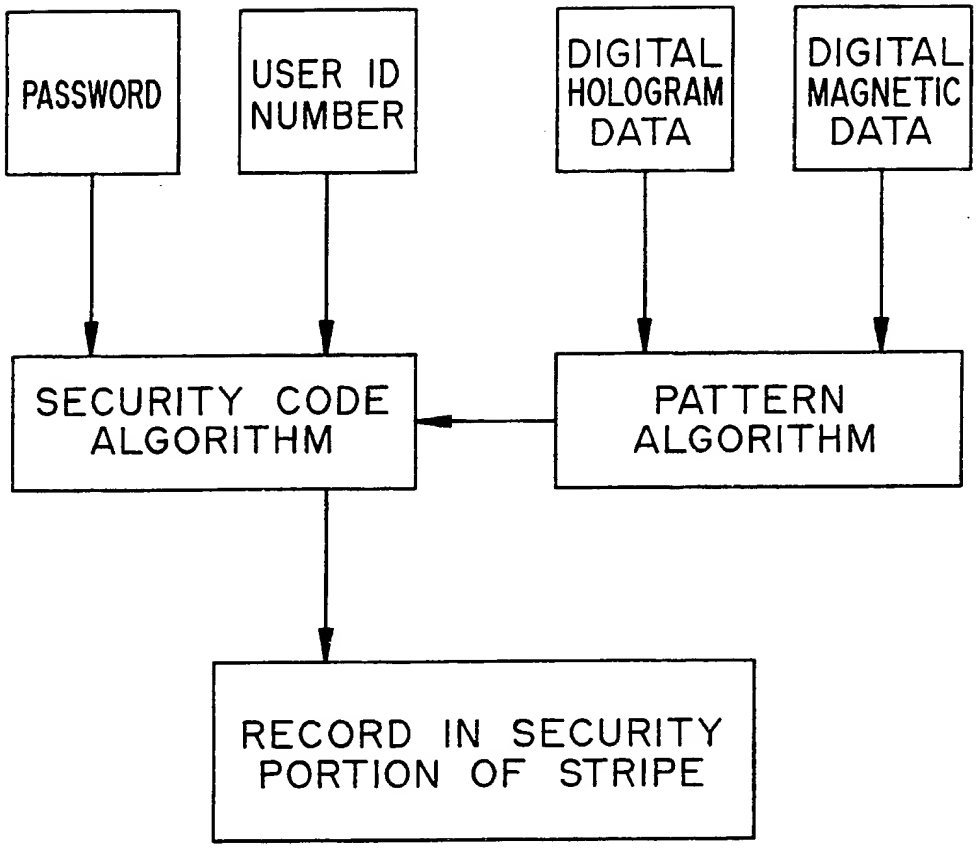


FIG. 9

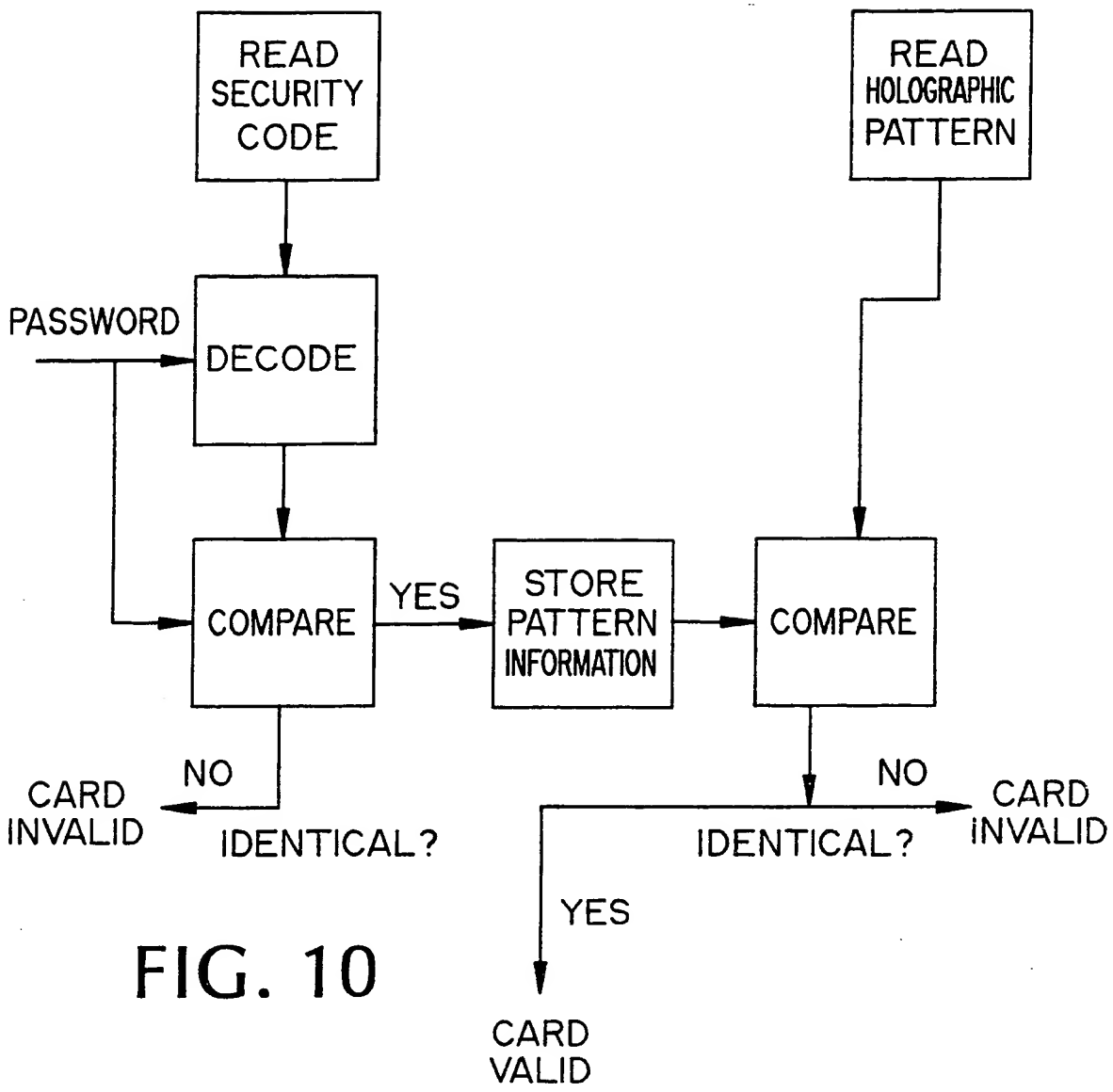


FIG. 10

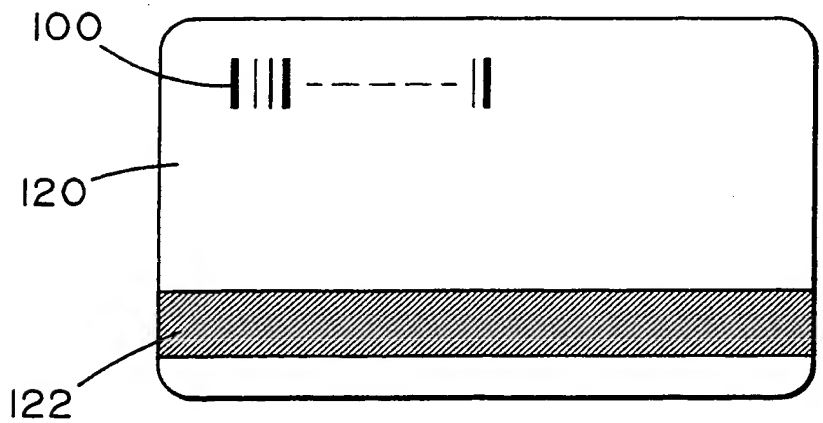


FIG. 11

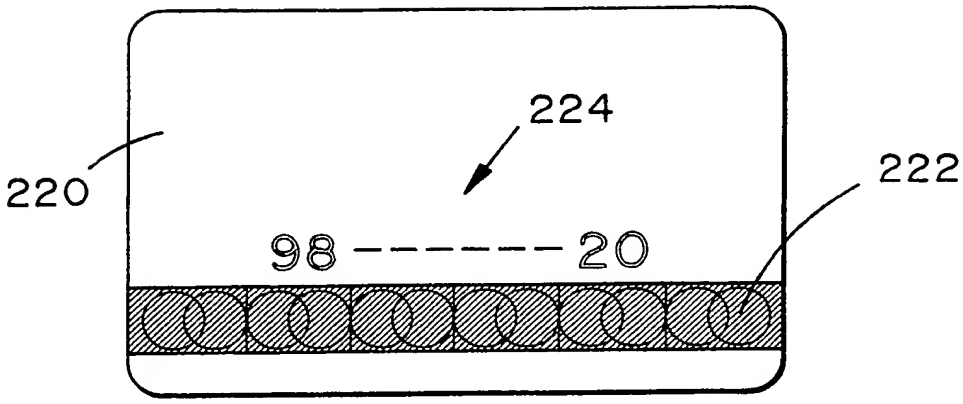


FIG. 12
(PRIOR ART)

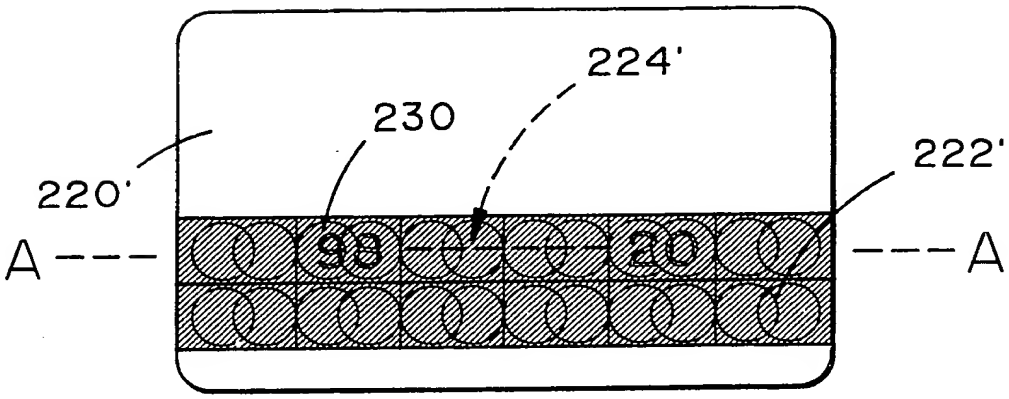


FIG. 13

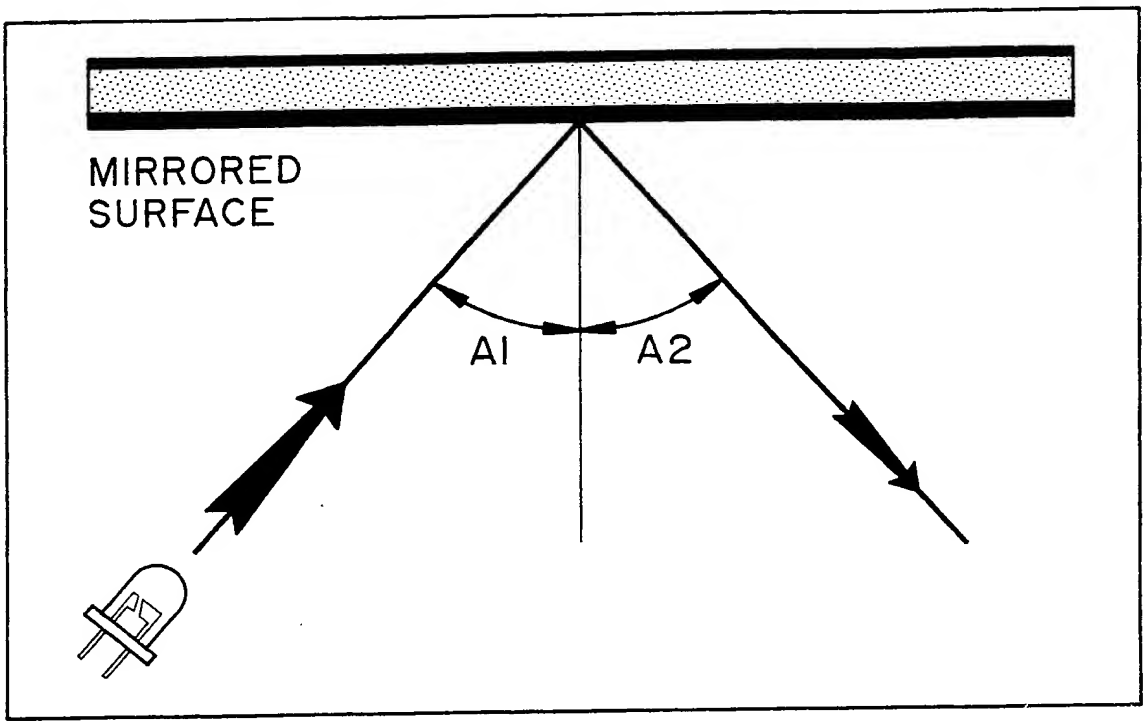


FIG. 14
(PRIOR ART)

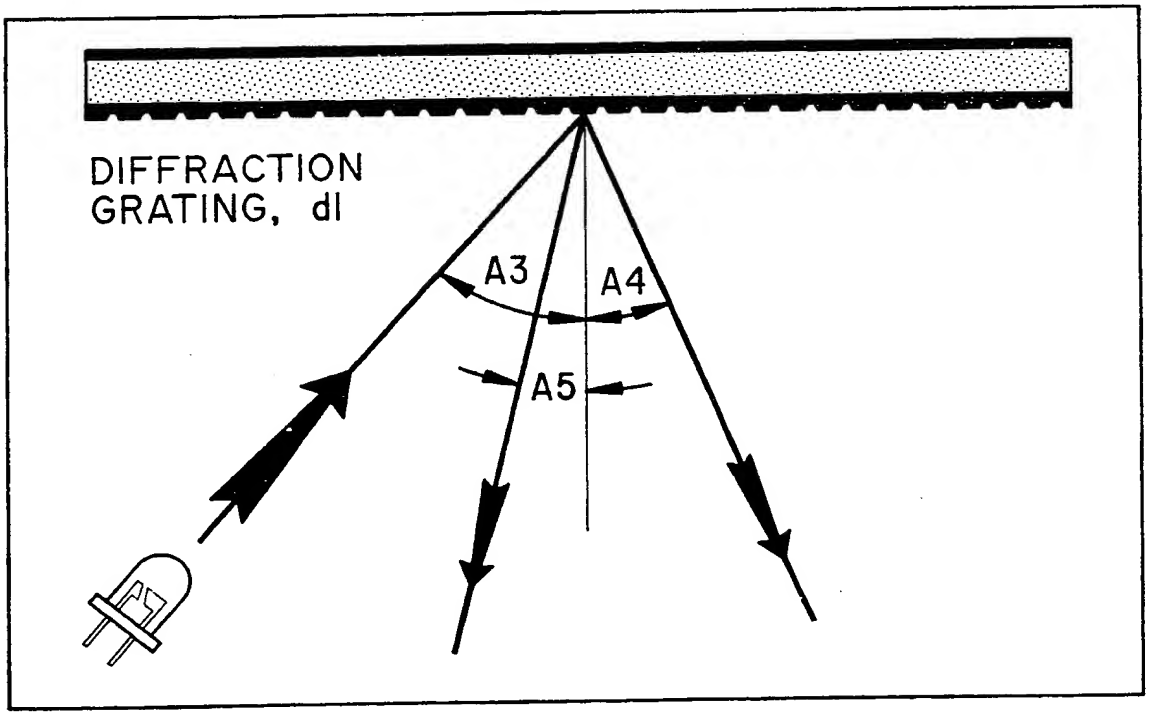


FIG. 15
(PRIOR ART)

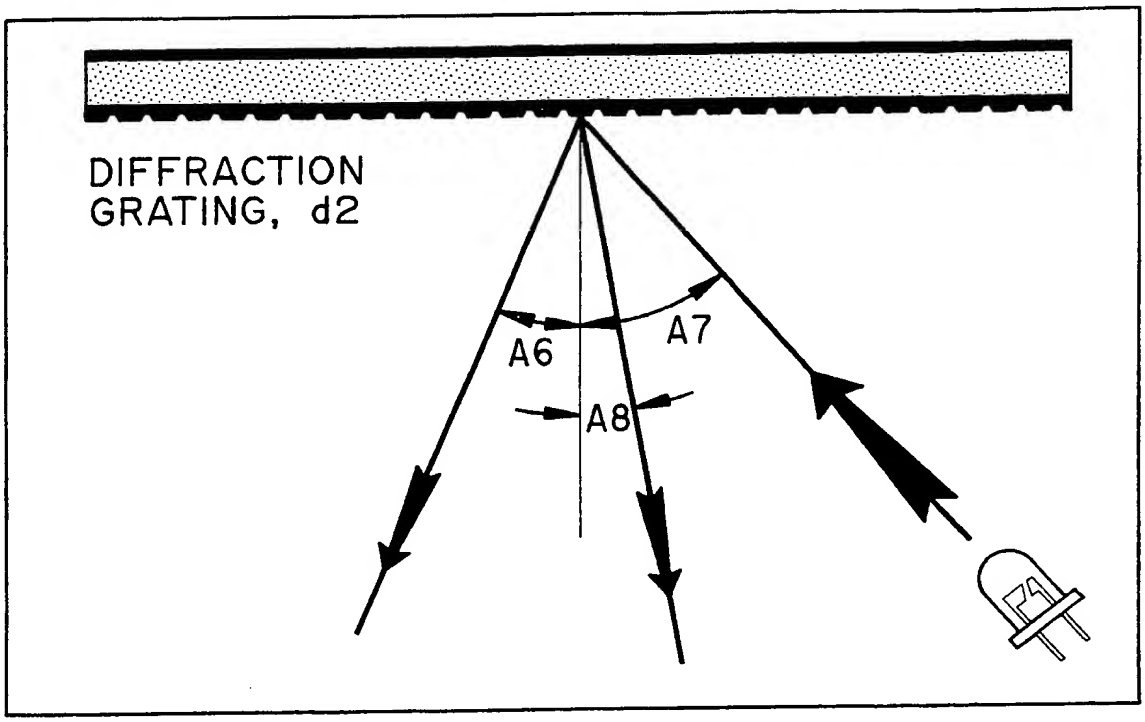


FIG. 16
(PRIOR ART)

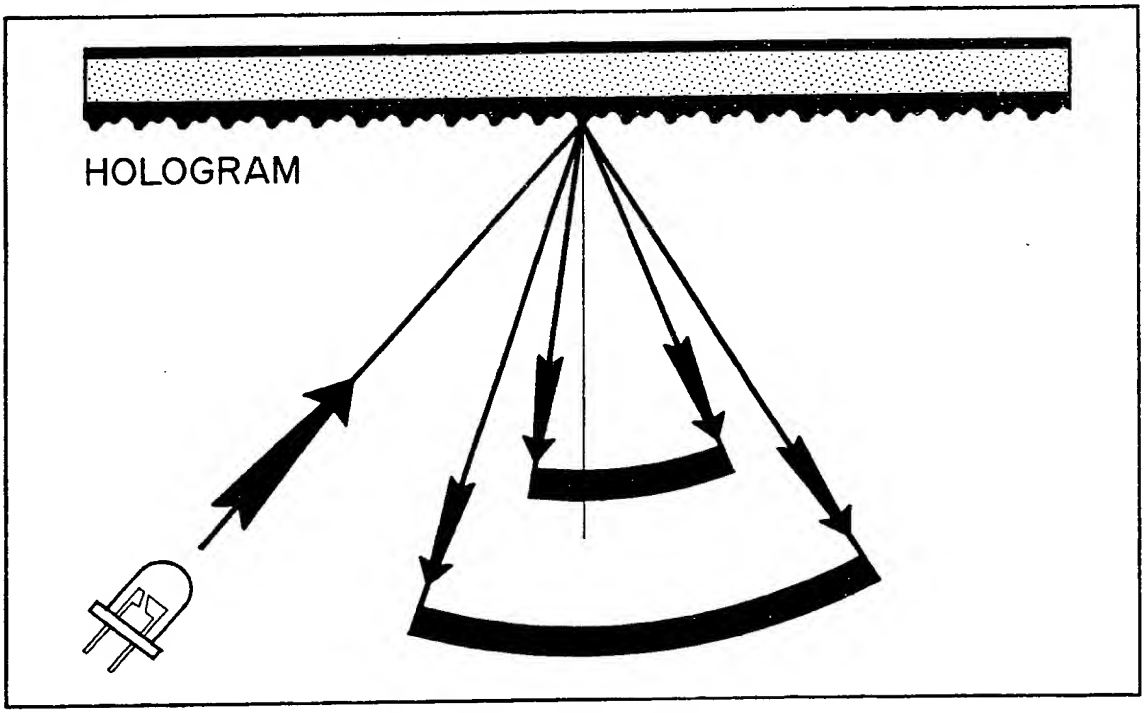


FIG. 17
(PRIOR ART)

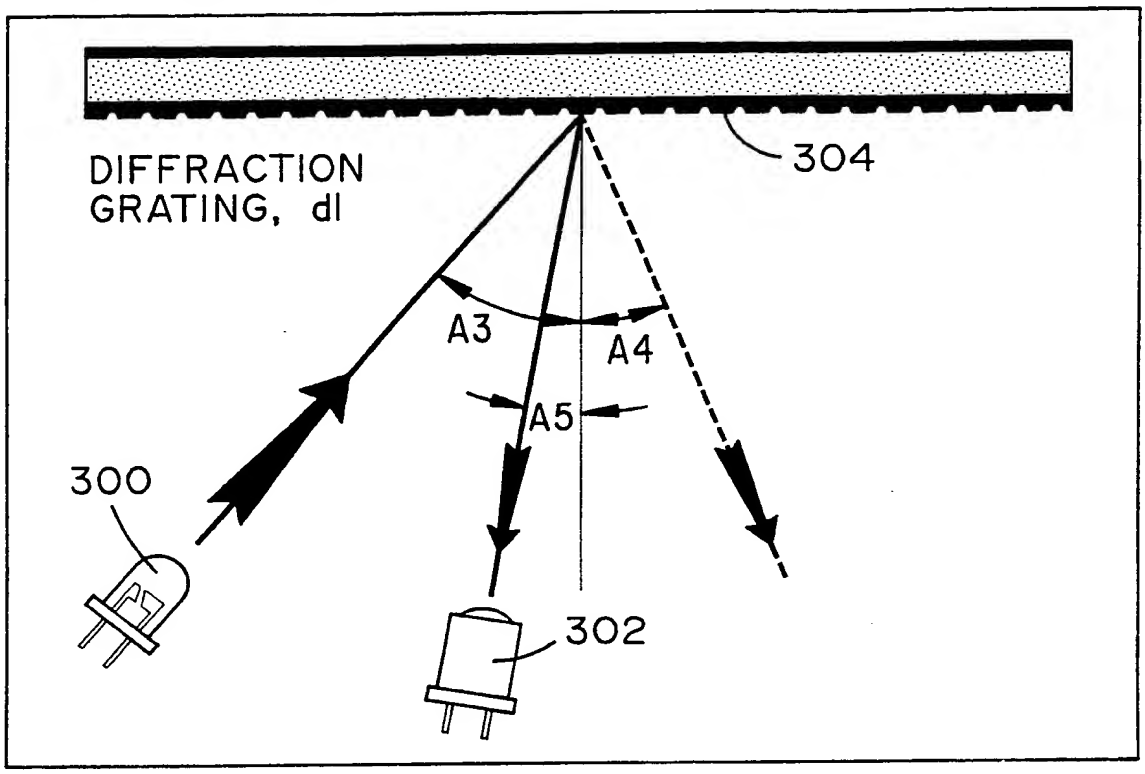


FIG. 18

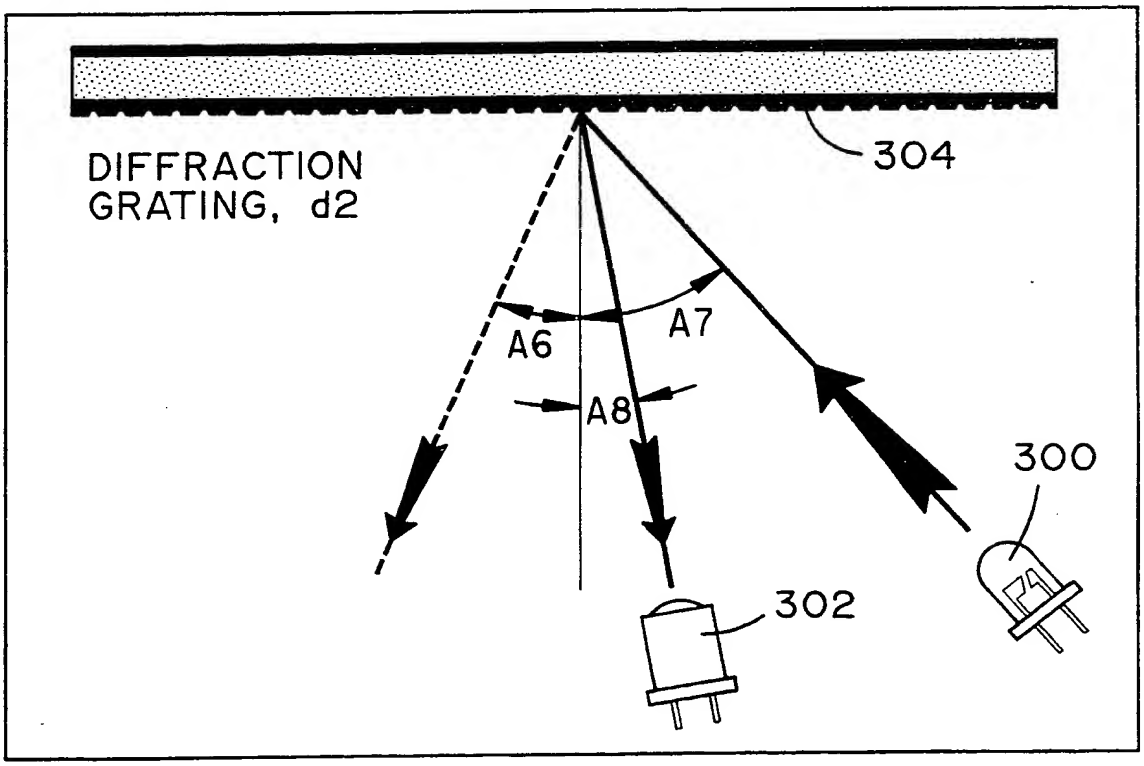


FIG. 19

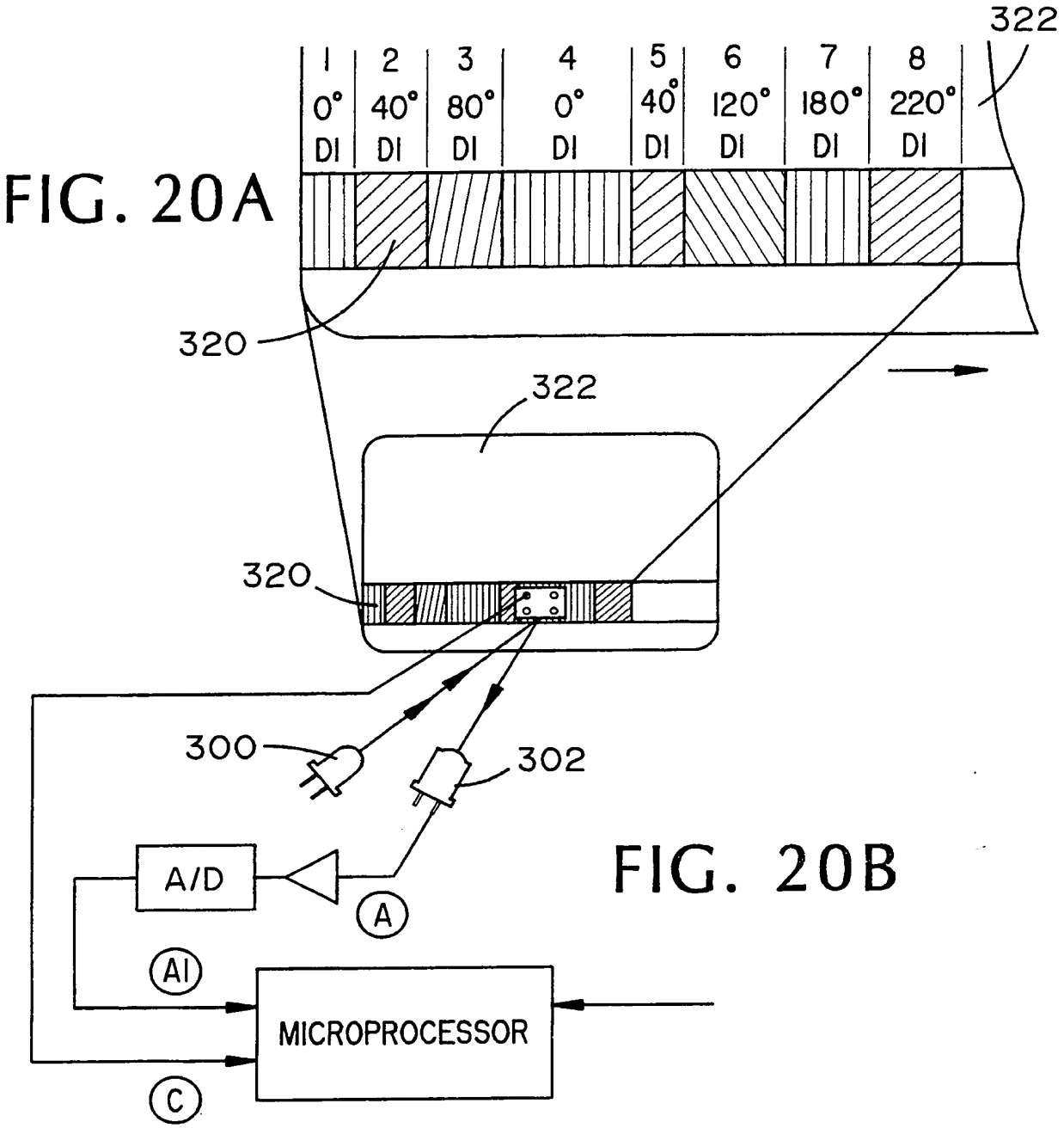


FIG. 20A

FIG. 20B

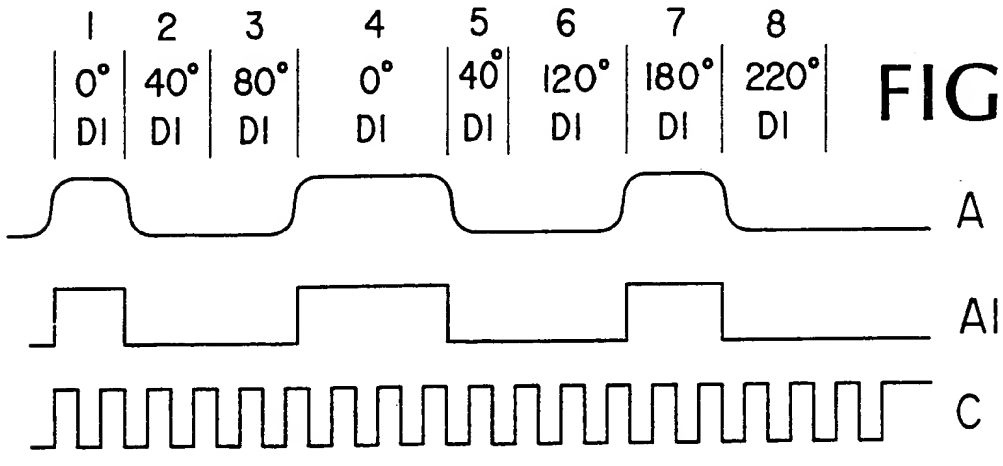


FIG. 20C

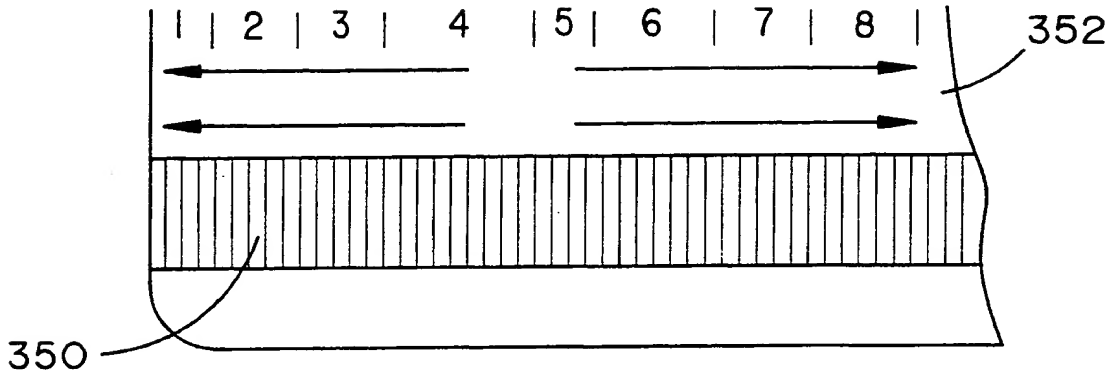


FIG. 21A

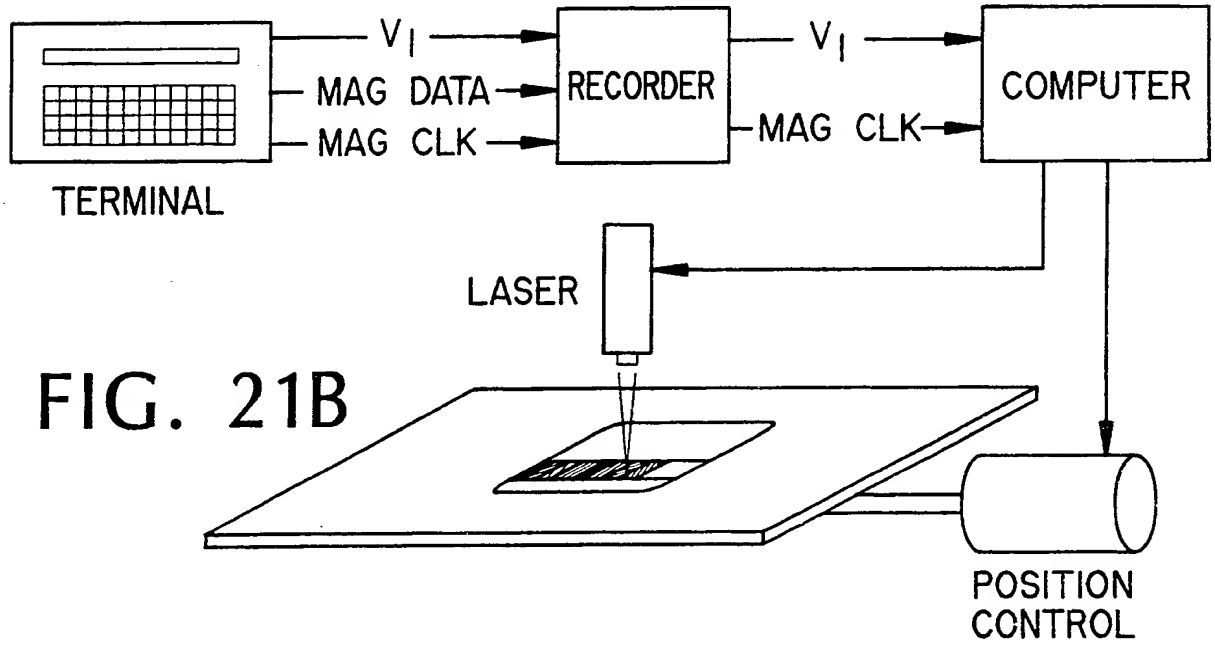


FIG. 21B

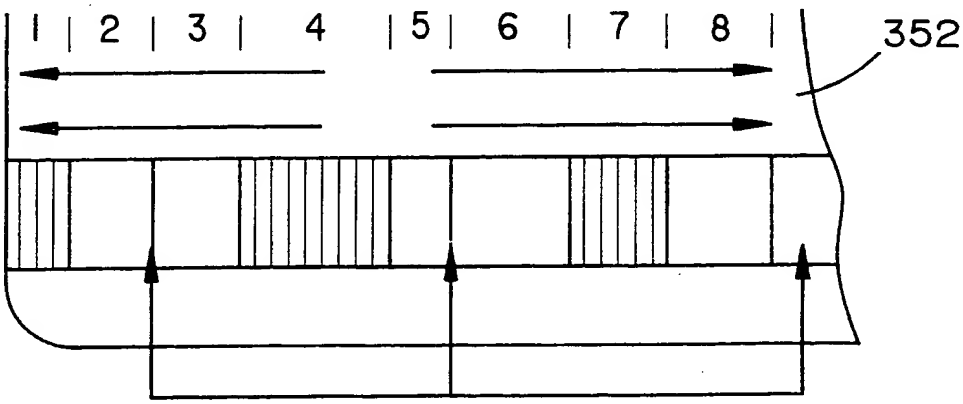


FIG. 21C

FIG. 22A

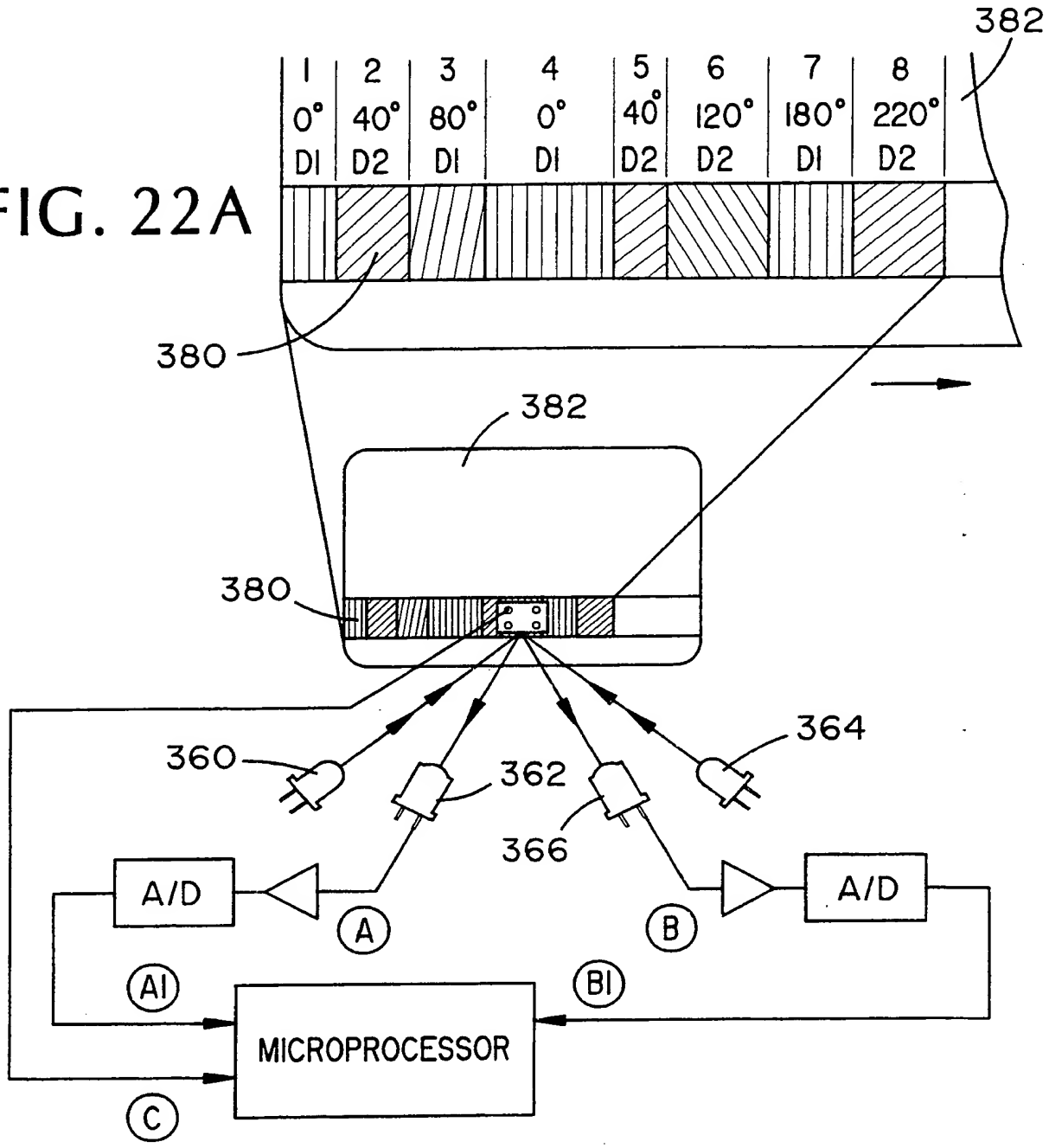


FIG. 22B

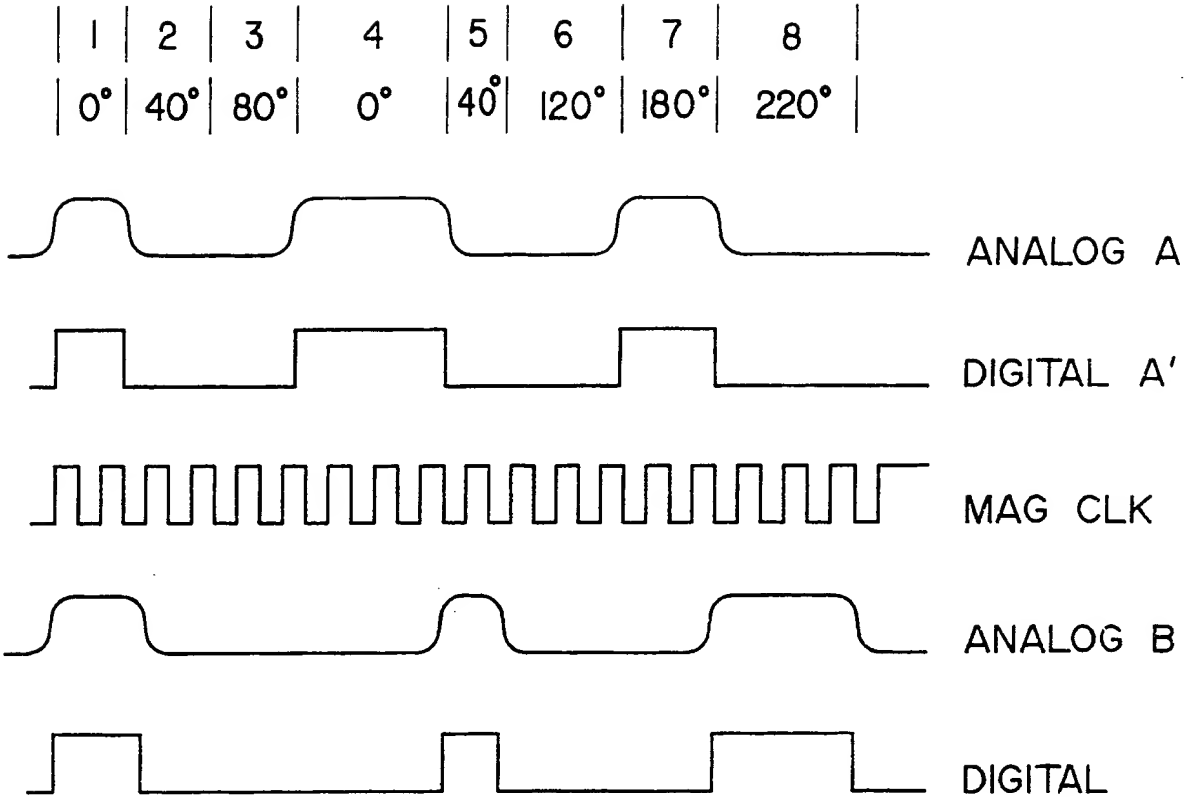
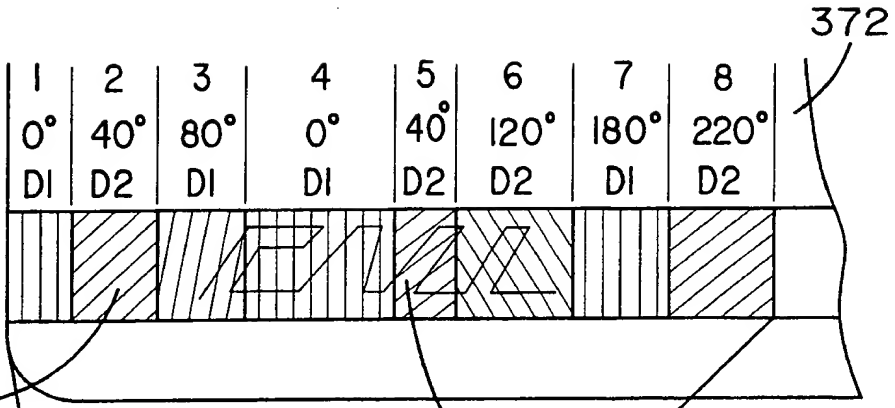


FIG. 22C

FIG. 23A



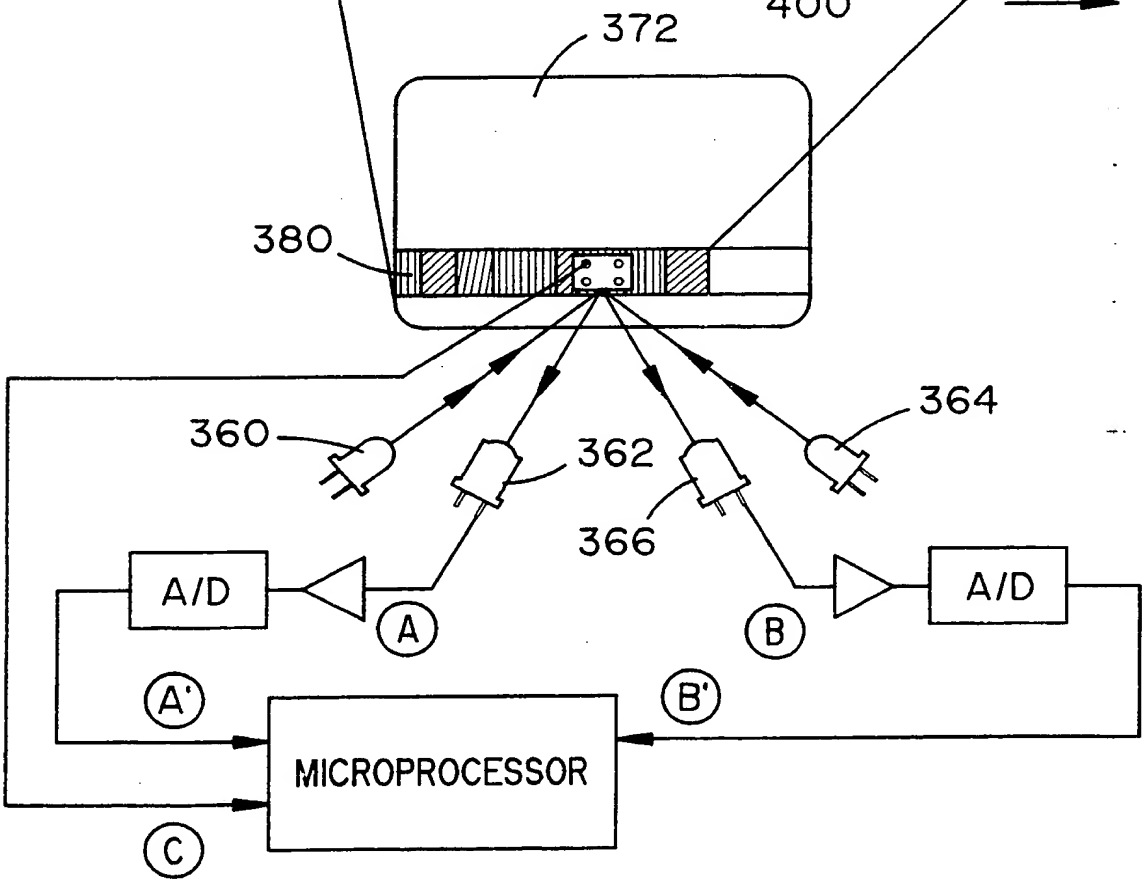


FIG. 23B

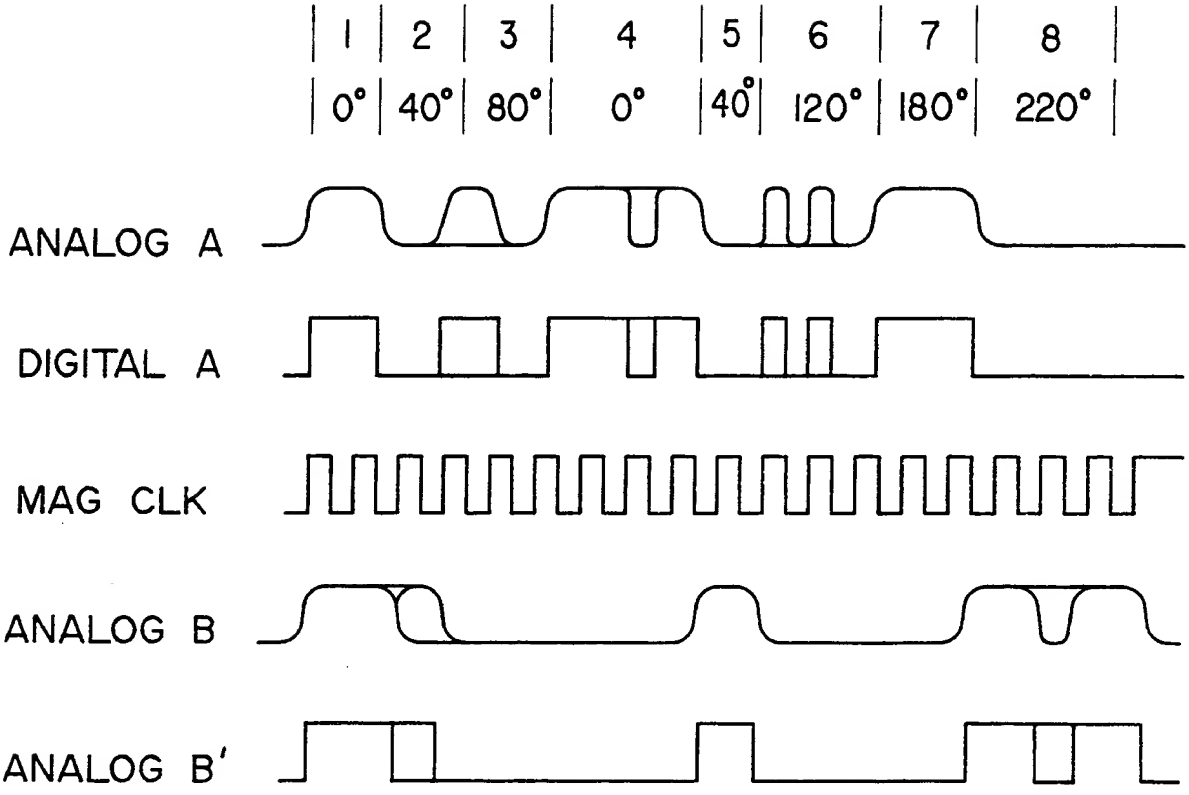


FIG. 23C

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US92/10357

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :G06K 7/08, 7/10, 19/12, 19/16
US CL :235/440,449,454,487,493
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 235/440,449,454,487,493 235/494; 283/86,91,904

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS U.S. and Jap. datafiles
search terms include card, magnetic, optical, spacial, relative distance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US,A, 4,013,894 (Foote et al.) 22 March 1977 See column 5, line 39 through column 6, line 7.	1-3,5,17 18,20 4,6-9,19 21-23
Y,P	US,A, 5,101,184 (Antes) 31 March 1992 See figure 3.	4,6-9,19 21-23
Y	US,A, 5,059,776 (Antes) 22 October 1991 See figures 1 and 4.	4,6-9,19 21-23
Y	US,A, 4,684,795 (Colgate, Jr.) 04 August 1987 See figure 1.	4
A	JP,A, 61-58092 (Comput Services Corp.) 25 March 1986 See Abstract, Fig. 2.	1,17

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 FEBRUARY 1993

Date of mailing of the international search report
08 APR 1993

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. NOT APPLICABLE

Authorized officer
EDWARD SIKORSKI

Telephone No. (703) 308-1297

Form PCT/ISA/210 (second sheet)(July 1992)*

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP,A, 63-91826 (Mitsubishi Heavy Ind. Ltd.) 24 April 1988 See Abstract, Fig. 3.	1,17
A	EP,A, 0,312,479 (Oberthur Card Systems) 19 April 1989 See Abstract, Fig. 1.	10,24
X	US,A, 4,211,918 (NYEFELER ET AL) 08 JULY 1980 See figures 9,11, and column 7, lines 41-47; column 3, lines 4-12.	11-13
X	US,A, 4,140,373 (RÜLL) 20 FEBRUARY1 979 See abstract	11-15
X	US,A, 4,250,393 (GREENAWAY) 10 FEBRUARY 1981 See fig 3, and abstract	11
A	US,A, 4,368,979 (RUELL) 18 JANUARY 1983 See fig. 3,9, and column 4, lines 21-25	11,16
A	US,A, 4,568,141 (ANTES) 04 FEBRUARY 1986 See figs. 1 and 6	11
A	US,A, 4,597,593 (MAURER) 01 JULY 1986 See fig. 2 and abstract	16

International application No.
PCT/US92/10357

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

I. Claims 1-10,17-24, drawn to a secure optomagnetic information system, classified in Class 235, Subclass 487.

II. Claims 11-16, drawn to an apparatus for reading an optically readable optical diffraction pattern, classified in Class 235, Subclass 454.

The two groups of invention do not share common features so as to constitute a single inventive concept. For example, Group I requires magnetic data in addition to optical data, while Group II is concerned only with optical data. Further, Group II is directed to an apparatus for reading the optical data, while Group I does not specifty the types of readers for the optical and magnetic data.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US92/10357

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.